La loi sur le renseignement du 25 juillet 2015 : "la France, État de surveillance" ?

MASTOR WANDA

Référence de publication : MASTOR (W.), « La loi sur le renseignement du 25 juillet 2015 : "la France, État de surveillance″ ? », Actualité juridique. Droit administratif , n° 36, 2015, p. 2018.

La loi sur le renseignement du 25 juillet 2015 : "la France, Etat de surveillance″ ?

L'essentiel

La loi sur le renseignement du 24 juillet 2015 a été qualifiée, par ses détracteurs, de « *Patriot Act* à la française ». L'objet de cette étude est de repousser cette comparaison, tout comme l'affirmation selon laquelle la France autoriserait les surveillances de masse, au moment même où les Etats-Unis, avec le récent *Freedom Act*, les interdiraient. La loi, indispensable dans son principe, n'est pas exempte de toute critique : l'option de finalités extrêmement larges et imprécises, tout comme « l'évacuation » de la question des surveillances internationales et le choix de l'autorisation préalable par une autorité non juridictionnelle n'emportent pas notre conviction. Un cantonnement à la lutte contre le terrorisme aurait permis d'entraîner la compétence d'un juge spécialisé, garantie plus efficace que ne l'est un avis simplement consultatif d'une nouvelle - et énième - autorité administrative indépendante.

Loi n° 2015-912 du 24 juillet 2015 relative au renseignement (JO du 26 juillet 2015, p. 12735)

Si le contexte n'était pas aussi grave, le titre de cet éditorial du *New York Times* (« *The French Surveillance State* », 1er avr. 2015) pourrait être qualifié d'ironique, tant il rappelle les termes utilisés par les observateurs français à l'époque de l'adoption, par des Etats-Unis traumatisés, de la loi anti-terroriste. L'auteur y rappelle que Manuel Valls « a assuré à la Nation que le texte proposé n'était pas un *Patriot Act* français », estimant ensuite que les parlementaires ne devraient pas le voter tant qu'un juge n'approuve pas ces surveillances, tous les pouvoirs lui semblant concentrés dans les mains des services du Premier ministre. Il n'est bien évidemment pas question d'accorder du crédit à cet article de presse, pas plus d'ailleurs qu'aux médias français qui, à la suite de l'adoption de la loi sur le renseignement le 24 juillet 2015, ont systématiquement comparé cette dernière aux lois américaines, sans nécessairement prendre la peine de les lire attentivement, la plupart du temps pour affirmer qu'elle allait « plus loin ». Mais tous sont révélateurs d'une certaine opinion, éclairée ou non. A l'instar des débats parlementaires ou des premiers commentaires doctrinaux, les journalistes n'échappent pas à la présentation binaire du débat relatif à la lutte contre le terrorisme en général et au renseignement en particulier : le choix entre la sécurité ou la liberté. Quels que soient les formules utilisées, le style employé, la problématique semble s'enfermer dans cette impasse, caricaturée par l'ajout de l'argument idéologique. Tout semble se passer, en France, comme si la gauche favorisait l'expression des libertés et la droite les questions de sécurité. Il est à cet égard décevant de constater, à la lecture des débats parlementaires, que nos représentants n'échappent pas à cette vision manichéenne du monde.

Dès la présentation générale du projet de loi, le Premier ministre a mis en garde contre tous « les fantasmes » qui entourent la question de la surveillance, insistant d'emblée sur le fait que celle-ci comporte de nombreux « garde-fous » dont l'autorisation préalable, le contrôle, le droit au recours juridictionnel effectif. Et Manuel Valls de préciser que « ceux qui n'ont pas compris cela n'ont pas lu le texte [...] ; certains raccourcis confinent, une fois encore, à la caricature » (Ass. nat., séance du 13 avr. 2015). Les

confusions, la méconnaissance ou les interprétations erronées des lois américaines, du *USA Patriot Act* (*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, Public Law*, 107-56) de 2001 au *USA Freedom Act* (*Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act, Public Law*, 114-23), adopté le 2 juin 2015, les incertitudes et les craintes caractérisent l'accueil réservé à la loi sur le renseignement. Un brouillard interrogatif que la décision du Conseil constitutionnel (23 juill. 2015, n° 2015-713 DC, AJDA 2015. 1513) n'a pas permis de dissiper ni - forcément car non encore installée - la nouvelle autorité administrative indépendante (AAI) créée par la loi. Sa composition vient d'être annoncée par le décret du Président de la République du 1er octobre 2015(1). En vertu de la loi organique relative à la nomination du président de la Commission nationale de contrôle des techniques de renseignement (CNCTR) (n° 2015-911 du 24 juill. 2015, jugée conforme par le Cons. const. dans sa décis. n° 2015-714 DC du 23 juill. 2015), la nomination, par le Président de la République, du président de ladite Commission a été confirmée par les commissions permanentes compétentes de chaque assemblée.

La loi peut être critiquée pour ce qu'elle contient, voire ce qu'elle ne contient pas, mais il faut au préalable repousser vigoureusement - et scientifiquement - l'affirmation selon laquelle elle serait le jumeau français du *Patriot Act* américain. Cette critique, abondamment relayée par certains médias, fut également au coeur de certaines interventions de nos représentants, du premier jour des débats (« Ce texte s'apparente bien à un *Patriot Act* à la française, quelles que soient les allégations du gouvernement, et même si on ne va pas aussi loin que les Américains », Ass. nat., H. Morin, séance du 13 avr. 2015) au dernier (« La loi sur le renseignement c'est, malgré tous les dénis, le camp du *Patriot Act* avec 14 ans de retard [...] », Ass. nat., J.-J. Candelier, séance du 24 juin 2015). Que les détracteurs regrettent que la loi soit adoptée au moment même où les Etats-Unis, réagissant aux révélations d'Edward Snowden, reviennent sur les dispositions les plus contestées du *Patriot Act* est une chose. Qu'ils la comparent avec ces dernières en est une autre.

Le fait que le projet soit porté et défendu par les socialistes n'a pas rassuré une partie des élus, électeurs, sympathisants de gauche, les associations de défense des libertés, tout comme il a soulevé de profondes craintes de la part de la Commission nationale de l'informatique et des libertés (délib. n° 2015-078 du 5 mars 2015 portant avis sur un projet de loi relatif au renseignement), du Défenseur des droits (avis n° 15-09 du 29 avr. 2015), de la commission de réflexion et de proposition sur le droit et les libertés à l'âge du numérique de l'Assemblée nationale et même du comité des droits de l'homme de l'ONU (obs. du 21 juill. 2015, CCPR/C/SR.3193). La première considère que « l'ensemble des dispositions permettra la mise en oeuvre de mesures de surveillance beaucoup plus larges et intrusives que ce qu'autorise le cadre juridique actuel en matière de renseignement » ; le second « regrette que les débats à l'Assemblée nationale n'aient pas abouti à un meilleur équilibre entre les impératifs publics de sécurité et la protection des droits et libertés ». Quant au comité des Nations unies, il souligne, quelques heures avant la décision du Conseil constitutionnel, que le texte octroie des « pouvoirs excessivement larges de surveillance très intrusive aux agences de renseignement ».

La recherche de l'équilibre, la conciliation, la balance des intérêts, le respect de l'absence de disproportion sont des opérations au coeur de l'activité délibérative des pouvoirs exécutif, législatif et judiciaire. Opérations délicates dans lesquelles la notion de seuil, même non explicitement avouée, est omniprésente. Jusqu'à quel point les libertés peuvent-elles être limitées au nom d'un intérêt supérieur ? A partir de quel moment le motif légitime permettant ces limitations bascule-t-il dans le domaine inacceptable de l'illégitime ? A partir de quand, très concrètement, la phase préventive de recherche de renseignements cède-t-elle la place à la phase d'enquête et de procédure judiciaires ? Quel est le critère permettant de

hisser une urgence au rang d'une urgence « absolue » ? La loi sur le renseignement, peut-être plus que toute autre, pose avec difficulté cette question de l'équilibre entre le respect des libertés et la sauvegarde de l'ordre public.

Personne ne remet en cause le fait que les interceptions de correspondances, les collectes de métadonnées, la pose d'algorithmes, de IMSI-*catchers*, de logiciel espions sont une atteinte au respect de la vie privée et à la liberté de communication. Tout comme personne ne remet en cause le fait que le terrorisme doit être combattu sous toutes ses formes. Il faut donc, pour commencer, sortir de l'impasse manichéenne énoncée plus haut (sécurité *vs.* liberté) et combattre l'idée selon laquelle les Français seraient divisés en deux camps : celui des pro-sécurité, laquelle est, comme le rappelle le premier article du code de la sécurité intérieure (CSI), « un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives », et celui des pro-libertés, qui n'auraient pas conscience de la réalité de la menace. Pour le dire autrement, à travers les mots des députés auteurs de la saisine du Conseil constitutionnel : « Il n'y a pas, d'un côté, ceux qui seraient déterminés à défendre la République et, de l'autre, le camp des naïfs ou des mauvais patriotes ». Même si, dans l'ensemble, la communauté politique a soulevé la nécessité du principe d'une telle législation, qui remédie aux « insuffisances », au caractère « lacunaire », à « l'approche fragmentée » du cadre légal antérieur pour reprendre les mots de son exposé des motifs, l'accueil est mitigé et exprime craintes et incertitudes.

Face à une loi de telle ampleur et à la décision du Conseil constitutionnel qui a suivi, le juriste doit tenter de se débarrasser de ses propres options partisanes, idéologiques voire philosophiques. Il doit tenter d'échapper au clivage classique qui envenime le débat plus qu'il ne le nourrit, en assumant les réflexions laudatives et critiques. Le recours au droit comparé lui permet d'évacuer l'argument d'autosatisfaction qui nous donnerait une sorte de label de qualité *a minima* (« nous n'allons pas aussi loin que les Etats-Unis ») et de mettre en évidence, pour mieux les confronter, proximités et divergences des lois concernées. Cette posture méthodologique est particulièrement utile pour l'étude de trois points saillants de la loi : la question de la finalité du renseignement, de ses techniques et du contrôle de sa mise oeuvre. La loi étant, à nos yeux, absolument nécessaire pour lutter contre une menace bien plus violente que ne l'est son contenu car exterminatrice de nos libertés et non seulement attentatoire, nous développerons essentiellement des arguments qui auraient permis à la loi d'échapper aux principales critiques, souvent légitimement fondées. Pour les trois points analysés, il existait des alternatives aux choix retenus qui nous paraissent plus adaptées.

I - Les finalités: au-delà de la seule lutte contre le terrorisme

Avant de rappeler les finalités de la loi récemment adoptée qui figurent à l'article L. 811-2 du CSI qu'elle modifie, il y a lieu d'indiquer d'emblée notre principale critique. Une limitation à la lutte contre le terrorisme aurait paru plus légitime, car plus urgente et précise. La plupart des parlementaires opposés à ce premier contenu, qu'il s'agisse des auteurs de la saisine du Conseil constitutionnel ou de tous ceux qui ont débattu de la loi tout comme les autorités ayant délivré un avis antérieur à son adoption, soulignent le caractère trop large, vague, imprécis de ses finalités assignées.

A. Le choix d'un champ d'application vaste et imprécis

De manière classique, la loi commence par rappeler que « l'autorité publique ne peut porter atteinte [au respect de la vie privée dans toutes ses composantes] que dans les seuls cas de nécessité d'intérêt public

prévus par la loi, dans les limites fixées par celle-ci et dans le respect du principe de proportionnalité ». Sont ensuite énumérées ces hypothèses justifiant l'atteinte portée aux libertés : « 1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ; 2° Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ; 3° Les intérêts économiques, industriels et scientifiques majeurs de la France ; 4° La prévention du terrorisme ; 5° La prévention : a) Des atteintes à la forme républicaine des institutions ; b) Des actions tendant au maintien ou à la reconstitution de groupements dissous [...] ; c) Des violences collectives de nature à porter gravement atteinte à la paix publique ; 6° La prévention de la criminalité et de la délinquance organisées ; 7° La prévention de la prolifération des armes de destruction massive ».

Plusieurs éléments militaient en faveur de la restriction de cette liste. Tout d'abord, son caractère imprécis qui paraissait également évident aux yeux des auteurs de la saisine du Conseil constitutionnel, qui soulignent une « sémantique trop relâchée », des termes si « flous » que la garantie des droits devient « illusoire ». Difficile, concrètement, de définir les atteintes portées à la forme républicaine des institutions, tout comme il est difficile de dénier le caractère démesurément englobant des « violences collectives de nature à porter gravement atteinte à la paix publique ».

Même si les promoteurs de la loi se sont défendus d'avoir réagi à l'actualité - d'où la procédure parlementaire accélérée - suite aux attentats terroristes perpétrés sur le sol français (v., not., en ce sens les propos de P. Nauche, rapporteur pour avis de la commission de la défense nationale et des forces armées au cours de la séance du 13 avr. 2015 à l'Ass. nat.), il paraît évident que ces derniers ont été l'un des principaux moteurs des travaux. Il faut néanmoins souligner que l'intérêt de Jean-Jacques Urvoas, auteur du substantiel rapport fait au nom de la commission des lois (Rapport fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, après engagement de la procédure accélérée, sur le projet de loi relatif au renseignement, doc. AN, n° 2697, 351 p.), pour les questions relatives au renseignement et sa volonté de clarifier cette opaque nébuleuse sont antérieurs aux attentats dits de Charlie hebdo et de l'hyper cacher (v. J.-J. Urvoas et P. Verchère, *Pour un « Etat secret » au service de notre démocratie*, rapp. d'information sur l'évaluation du cadre juridique applicable aux services de renseignement, doc. AN n° 1022, 14 mai 2013, 205 p. ; J.-J. Urvoas, Rapport fait au nom de la commission d'enquête sur le fonctionnement des services de renseignement français dans le suivi et la surveillance des mouvements radicaux armés, doc. AN n° 1056, 24 mai 2013, 163 p.). Mais, au lieu d'avancer l'argument d'une loi non exclusivement cantonnée à la lutte contre le terrorisme, et tout en continuant d'afficher la volonté de fournir un cadre légal clair aux activités des services de renseignement, il aurait peut-être été plus pertinent de restreindre son champ d'application pour la seconde raison suivante : les enseignements tirés de l'expérience américaine.

B. Les enseignements de l'expérience américaine

Quand le *Patriot Act*, acronyme soigneusement réfléchi, fut voté au lendemain des attaques du 11 septembre, les observateurs étrangers - à commencer par l'auteur de ces lignes (L'état d'exception aux Etats-Unis : le *USA Patriot Act* et autres violations "en règle" de la Constitution, *Annuaire International de Justice constitutionnelle*, t. 24, 2008. p. 461-475) - se sont indignés de son aspect liberticide. L'ampleur de cet événement, sans précédent, va servir à justifier la guerre que George W. Bush entend mener contre « l'Axe du Mal » (discours sur l'état de l'Union du 29 déc. 2002) : le 14 septembre, il déclare l'état d'urgence nationale et signe un décret soumettant les forces armées de réserve à un régime d'activité. Dans les jours qui vont suivre, une loi de plus de 300 pages est adoptée à une écrasante majorité, qui modifie notamment

la loi de surveillance d'intelligence étrangère (*Foreign Intelligence Surveillance Act* [FISA]) de 1978.

Le contenu du *USA Patriot Act* est en conflit tant avec des droits substantiels que processuels. De manière générale, de nouveaux dispositifs de surveillance sont créés ; les mesures d'interception des communications, auparavant cantonnées à des situations exceptionnelles, sont généralisées. Au total, six amendements de la Constitution sont mis à mal par le dispositif anti-terroriste. Il faut isoler, pour l'intérêt de notre démonstration, l'ancienne section 802, qui donnait une définition particulièrement large du champ d'application de la loi via celle de l'activité terroriste. La notion de « terrorisme intérieur » (*domestic terrorism*) était liée à toute activité mettant en danger des vies humaines sur le territoire national et « visant à intimider la population civile ou infléchir la politique du gouvernement par le biais de destruction massive, d'assassinats ou d'enlèvements [...] ». L'imprécision d'une telle définition présentait l'inconvénient d'englober des actions étrangères au terrorisme au sens habituel. Et cette imprécision - sans doute volontaire - des termes a entraîné, fatalement, des abus dans les faits. En raison des termes employés, ce dispositif censé être spécifique pouvait tout aussi bien être utilisé dans le cadre d'affaires de droit commun, et il l'a effectivement été. Par le biais d'une interprétation extensive, toute protestation à caractère politique pouvait ainsi être qualifiée de « terrorisme intérieur », alors que le premier amendement interdit notamment au Congrès de voter des lois « restreignant la liberté de parole ». Selon les associations de défense des libertés, notamment la puissante ACLU (*American civil liberties union*), le FBI aurait utilisé à outrance cette possibilité offerte par la section 802, sans la limiter aux cas de terrorisme.

Les craintes, face à une définition si large du champ d'application de la loi française, sont donc fondées au regard des enseignements du droit comparé. Et il serait bien naïf de nous répondre que nos services de renseignement ne sont pas le FBI : y compris en France, des dispositions potentiellement dangereuses peuvent échapper un jour aux bonnes intentions de ses créateurs(2).

II - Les techniques : faut-il craindre une surveillance de masse ?

Le CSI comporte désormais un titre V intitulé : « Des techniques de recueil de renseignement soumises à autorisation », utilisées par des services qui seront désignés par décret en Conseil d'Etat (art. L. 811-2). Il faut préciser au préalable que l'article L. 821-7 exclut du recours aux techniques de renseignement les parlementaires, magistrats, avocats et journalistes. Invité à se prononcer sur l'absence des enseignants-chercheurs de cette liste, le Conseil constitutionnel a répondu par la technique explicative du « pourquoi ? Parce que » : « Considérant [...] que le principe d'indépendance des enseignants-chercheurs n'implique pas que les professeurs d'université et maîtres de conférences doivent bénéficier d'une protection particulière en cas de mise en oeuvre à leur égard de techniques de recueil de renseignement dans le cadre de la police administrative » (consid. 36). L'auditoire devra se contenter de cette « motivation » mais il convient de souligner que les mandats et professions protégés le sont pour la place qu'ils occupent au sein du débat public. Or les cours des enseignants-chercheurs ne sont pas délivrés dans un huis-clos confiné et secret. Les amphithéâtres, et plus encore les conférences et interventions dans des colloques, font de l'enseignant-chercheur un acteur clef dans la transmission du savoir et la formation de l'opinion publique. Ajoutons que c'est lui que les pouvoirs publics sont venus chercher pour parler de l'intégration dans les préfectures, de la laïcité dans les écoles, pour former certains imams et créer des diplômes d'université sur les religions. Et le constitutionnaliste comparatiste utilise nécessairement les moteurs de recherche qui pourraient être à présent considérés comme « suspects ». Il va de soi qu'un spécialiste de la lutte contre le terrorisme navigue sur les sites internet qui lui permettent de saisir les multiples facettes de l'objet de ses recherches...

A. Des techniques sophistiquées

Il s'agit concrètement des interceptions de sécurité (art. L. 852-1 I), de la sonorisation de certains lieux et véhicules et de la captation d'images et de données informatiques (art. L. 853-1 I), mais aussi, plus largement, du recueil, auprès d'opérateurs et d'hébergeurs, d'informations ou de documents portant sur les communications électroniques (art. L. 851-1 et L. 851-2). L'article 5 de la loi introduit, dans le CSI, les articles L. 851-1, L. 851-2, L. 851-3 et suivants qui permettent la collecte de ce qu'il convient d'appeler les « métadonnées ». Pour les détracteurs de la loi, la collecte de ces dernières serait encore plus attentatoire aux libertés que les données elles-mêmes. En résumé, ce n'est plus seulement le contenu d'un email qui est collecté mais toutes les informations qui lui sont relatives : l'adresse, l'heure et le support de l'envoi, etc. La collecte des métadonnées n'est en réalité ni moins ni plus intrusive que celle des données elles-mêmes, tant il est difficile de dissocier les deux. L'article L. 851-3 I permet par ailleurs la mise en place des fameuses « boîtes noires algorithmiques » et l'article L. 851-6 I les poses des IMSI-*catchers*, fausses antennes qui permettent d'intercepter les conversations téléphoniques. Bien évidemment, les téléphones situés à proximité de la cible sont susceptibles de se connecter à cette « borne-leurre ».

Le citoyen aura du mal à trouver dans la loi des explications relatives à ces techniques modernes et sophistiquées. Les boîtes noires ont été particulièrement dénoncées pendant les débats parlementaires, en raison de la surveillance de masse qu'elles permettraient. Or, nous y reviendrons, les détracteurs de la loi confondent *surveillance* et *collecte de masse*. Leur objectif est de détecter, grâce aux informations transitant par diverses infrastructures, des terroristes mais aussi leurs soutiens parmi la masse des internautes. Dans un langage plus technique, il s'agit, pour les services de renseignement, de repérer les individus qui se cacheraient dans la masse, en analysant l'ensemble du trafic qui transite par les opérateurs, de façon indiscriminée. Les députés auteurs de la saisine du Conseil constitutionnel ont pointé non seulement l'inconstitutionnalité d'une telle technique au regard du principe de proportionnalité mais également son inefficacité. Selon certains experts cités par les requérants, cette pratique engendrerait trop de « faux positifs », c'est-à-dire un pourcentage élevé de faux suspects. Il suffit de reprendre notre exemple cité plus haut du chercheur comparatiste qui, pour les besoins d'une recherche, consulterait régulièrement les sites internet considérés comme suspects.

Initialement, l'article L. 854-1 du CSI concernait également les mesures de surveillance internationale que les autorités françaises auraient été habilitées à mettre en oeuvre pour des communications émises ou reçues en dehors du territoire national. Chacun sait - ou peut imaginer - l'importance de telles surveillances pour la lutte contre le terrorisme. Surveillances encore permises aux Etats-Unis sous l'empire actuel du *Freedom Act*, qui n'est pas revenu sur la section 702 de la loi FISA. Celle-ci autorise toujours la *National Security Agency* (NSA) à espionner les communications qui entrent ou sortent du territoire américain. Les associations de défense des libertés avaient espéré que la nouvelle loi sur le renseignement abroge cette disposition, qui expire fin 2017. Ces mesures sont donc particulièrement délicates : or, et contrairement à ce que le législateur a fait pour les mesures de surveillance nationale, les conditions de mise en oeuvre des techniques de renseignement sont renvoyées par la loi française à un décret en Conseil d'Etat. Le Conseil constitutionnel a très logiquement censuré cette disposition, et l'argument parfois avancé de l'urgence dans laquelle les pouvoirs publics auraient travaillé - que nous réfutons par ailleurs - paraît ici pertinent. Le renvoi à un simple décret en Conseil d'Etat des conditions d'exploitation, de conservation et de destruction des renseignements collectés, des conditions de traçabilité et de contrôle par la commission nous paraît tout simplement incompréhensible. Le législateur a rapidement réagi en proposant un nouveau texte, qui

vient d'être adopté en première lecture par l'Assemblée nationale (proposition de loi relative aux mesures de surveillance des communications électroniques internationales, Ass. nat., texte adopté n° 590, 1er oct. 2015), encadrant intégralement ces surveillances internationales, sans renvoi à un décret en Conseil d'Etat.

La question de la durée de détention de ces données et métadonnées a également été au coeur des travaux préparatoires de la loi. Leur récolte est, comme nous le verrons plus loin, placée sous l'autorité du Premier ministre qui « organise la traçabilité de l'exécution des techniques autorisées [...] et définit les modalités de la centralisation des renseignements collectés » (art. L. 822-1, al. 2). Concrètement, une technique de recueil de renseignements mise en oeuvre fait l'objet d'un relevé indiquant les dates de début et de fin de la collecte, de même que la nature des renseignements collectés. Initialement, le projet de loi prévoyait que les données recueillies seraient détruites au terme d'un an à compter de leur recueil, durée maximale réduite à un mois pour les interceptions de sécurité, ou portée à cinq ans pour les données de connexion. Le travail parlementaire fut sur ce point capital, les délais courant finalement non dès le *recueil* des informations mais dès le moment de leur *exploitation*. Ils seront de trente jours pour les correspondances interceptées et pour les paroles captées, de quatre-vingt-dix jours pour les renseignements collectés grâce à une sonorisation, prise d'image ou une captation de données informatiques ; enfin, ils seront de cinq ans pour les données de connexion.

Lors des débats parlementaires, il a souvent été avancé que la France légalisait la surveillance de masse au moment même où les Etats-Unis l'interdisaient. C'est non seulement inexact mais faux.

B. Surveillance de masse ou collecte de masse ?

Le *Freedom Act* et la loi française sur le renseignement ne permettent pas la surveillance de masse mais la collecte de masse. La subtilité réside dans la question de l'utilisation des données collectées, en amont, par les divers opérateurs. Mais l'autorité, quelle qu'elle soit (FBI et NSA aux Etats-Unis, le Premier ministre en France), ne pourra désormais accéder auxdites données que si la demande est ciblée, d'une part, et entourée de plusieurs garanties (autorisation par un juge ou une autorité), d'autre part.

« L'adoption du projet de loi favorisera la progression de l'Etat de droit. En effet, le texte n'instaure absolument aucune surveillance de masse. Il propose même de faire exactement le contraire en ne prévoyant que des surveillances ciblées », a dû préciser Philippe Bas, le rapporteur pour le Sénat de la commission mixte paritaire (séance du 23 juin 2015). Le ministre de l'intérieur s'est défendu, le même jour, avec véhémence d'instaurer un contrôle de masse : « Je veux insister fortement sur le fait que toutes les mesures du texte, sans aucune exception, procèdent du ciblage, de l'intentionnalité clairement manifestée et jamais - je dis bien jamais ! - du contrôle de masse [...]. Nous sommes contre la captation massive d'informations ! ». Bernard Cazeneuve a sans doute voulu éloigner le spectre orwellien des discours relatifs à la loi sur le renseignement. Mais de collecte de masse, il en est bien question, non par les services du Premier ministre mais par les opérateurs. Il en va à peu près de même aux Etats-Unis, qui ont banni les « *bulk collection* » (les collectes « en vrac ») opérées par les agences de surveillance.

Il faut commencer par relever que l'accueil du *Freedom Act*, adopté puis promulgué par le président Obama très peu de temps avant la loi française sur le renseignement, est plutôt positif pour une raison simple : il est pratiquement impossible, en théorie et en pratique, d'être plus attentatoire aux libertés que ne le fut la loi de 2001. Par 67 voix contre 32, le Sénat a donc adopté une loi qui limite les pouvoirs de surveillance de la NSA, le symbole de la recherche de l'acronyme *« Freedom »* étant tout aussi significatif

que ne l'était celle de *« Patriot »*, dans un contexte différent. Même si les Etats-Unis sont toujours engagés dans une guerre contre le terrorisme, selon les discours récurrents de l'exécutif, ce sont plutôt les révélations d'Edward Snowden qui ont motivé la préparation de cette récente loi (même si, contrairement à la loi française, la loi américaine n'a pas légalisé le statut de lanceur d'alerte). Il est faux d'affirmer que la loi de 2015 abroge et remplace celle de 2001. Certaines dispositions sont arrivées à expiration et, au lieu d'être supprimées, ont été remplacées ; d'autres ont été prolongées. En se fondant légalement sur les pouvoirs octroyés par le *Patriot Act*, les Etats-Unis avaient mis en place un système de surveillance généralisée.

En effet, la section 215 de la loi de 2001, intitulée « Accès à certaines archives commerciales en rapport avec la lutte contre l'espionnage et le terrorisme international », autorisait le gouvernement à obtenir de la part d'un tribunal secret (la *FISA Court*) la saisie des bases de données de toutes sortes d'institutions, y compris les bibliothèques. Ce que l'on appelait également « la clause bibliothèque » permettait avec une étonnante facilité l'intrusion des autorités gouvernementales dans la sphère personnelle de l'individu : les agents du FBI pouvaient demander un mandat dans le but d'obtenir des dossiers médicaux, financiers, des communications électroniques (SMS, mails) et téléphoniques, des informations sur les vidéos louées et les livres empruntés aux bibliothèques. Cette section 215 était de plus assortie de la clause dite « du bâillon » (*Gag Order*) interdisant à quiconque de révéler l'utilisation par le FBI de ladite section. Outre la collision avec le quatrième amendement de la Constitution, protégeant le « droit des citoyens d'être garantis dans leurs personne, domicile, papiers et effets, contre des perquisitions et saisies déraisonnables [...] », la section 215 allait à l'encontre d'une série de lois sur la confidentialité des fichiers de bibliothèques qui avaient été adoptées par les Etats suite à des abus perpétrés par le FBI.

Il convient d'ailleurs de préciser que l'obligation d'un mandat était somme toute récente : le *Protect America Act* du 5 août 2007, ironiquement rebaptisé le *Police America Act* par l'ACLU, avait modifié la loi FISA en donnant de nouveaux pouvoirs à la NSA. Cette dernière, autorisée à surveiller, sans mandat, toutes les communications en provenance ou à destination des Etats-Unis a largement utilisé cette faculté. Des révélations publiées à la une du New York Times le 16 décembre 2005 ont fait état de milliers d'écoutes extrajudiciaires effectuées au lendemain du 11 septembre. Suite à ces abus, la loi FISA a de nouveau été amendée par le *FISA Amendments Act* du 10 juillet 2008, qui « réhabilite » l'obligation du mandat et rend obligatoire l'aval de la *FISA Court* pour écouter un Américain à l'étranger alors que l'approbation de *l'Attorney general* suffisait auparavant.

C'est donc la volonté de limiter les pouvoirs de la NSA qui a clairement motivé le Président et le législateur américains. Les opérateurs de télécommunications, désormais, collecteront eux-mêmes les métadonnées de leurs clients (v. le titre I^{er} de la loi, « *FISA business records reform*s »). Le *Freedom Act* ne sonne donc pas le glas de la collecte de données qui pourront ensuite être délivrées au FBI ou la NSA, sous réserve d'une autorisation préalable de la *FISA Court* et de l'identification d'une cible précise. C'est par conséquent la fin des collectes massives, y compris des données de connexion internet, mais seulement en ce qui concerne les Américains...

De la collecte de masse à la surveillance de masse, il n'y a qu'un pas que les législateurs américain et français ont cherché à empêcher à travers la question, fondamentale, des garanties.

III - Les garde-fous : autorisations administratives et recours juridictionnels

Le juriste français n'est pas le seul à être habitué à l'argument classique, en matière de libertés, du « si et seulement si ». Les techniques de renseignement portant évidemment atteinte au respect de la vie privée et à ses composantes, elles doivent être soigneusement entourées de toute une série de garanties, dont certaines, telles que l'objectif ou la durée de conservation, ont déjà été évoquées. Les débats parlementaires, tournant parfois aux TD de droit constitutionnel (« Avez-vous déjà lu l'article 66 ? », « Savez-vous faire la différence entre un contrôle préventif et une action répressive ? », « A quoi sert un procureur ? ») se sont également, sans surprise, focalisés sur la question du statut des garde-fous et de leur compétence. La loi instaure une nouvelle AAI, censée encadrer les actions du Premier ministre en amont. Elle donne par ailleurs compétence au Conseil d'Etat pour recueillir d'éventuels recours en premier et dernier ressort. Nous étions, pour notre part, favorable à la compétence d'une autorité juridictionnelle unique.

A. Le choix français du « couple » AAI/Conseil d'Etat

La compétence de la CNCTR découle d'un syllogisme *a priori* imparable : la finalité du renseignement est notamment la préservation de l'ordre public ; il relève donc du champ de la police administrative ; autorités administratives et juge administratif sont donc compétents. Ceux qui se sont opposés à ce point précis de la loi ont avancé un autre syllogisme : la loi, compte tenu de ses finalités et des techniques mises en oeuvre, est une atteinte particulièrement violente aux libertés individuelles ; elle entre donc dans le champ d'application de l'article 66 de la Constitution ; elle entraîne donc la compétence du juge judiciaire. Le Conseil constitutionnel a tranché en faveur de la première position, rappelant que « le législateur s'est fondé sur l'article 21 de la Constitution pour confier au Premier ministre le pouvoir d'autoriser la mise en oeuvre des techniques de recueil de renseignement dans le cadre de la police administrative » (consid. 18).

Le législateur a fait de l'avis de la CNCTR (qui sera composée de deux députés, deux sénateurs, deux membres du Conseil d'Etat, deux magistrats hors hiérarchie de la Cour de cassation et d'une personnalité qualifiée pour sa connaissance en matière de communications électroniques) une garantie de leur mise en oeuvre. Or - et les opposants à la loi n'ont pas manqué de le soulever inlassablement -, cet avis préalable n'est que consultatif. Cette caractéristique n'a pas « ému » le Conseil constitutionnel qui s'est borné à répondre « qu'*en elle-même*, la procédure d'autorisation par le Premier ministre après avis de la Commission nationale de contrôle des techniques de renseignement ne méconnaît ni le droit au respect de la vie privée ni l'inviolabilité du domicile ni le secret des correspondances » (consid. 19, souligné par nous).

Bien sûr, les défenseurs de la loi ont rétorqué tout aussi inlassablement que le nouvel article L. 311-4-1 du code de justice administrative attribuait au Conseil d'Etat la compétence, en premier et dernier ressort, pour juger des requêtes concernant la mise en oeuvre des techniques de renseignement. Par ailleurs, le Conseil d'Etat pourra être saisi par toute personne souhaitant vérifier qu'elle ne fait pas - ou n'a pas fait - l'objet d'une surveillance irrégulière, et par la CNCTR qui estimerait que ses avis ou recommandations n'ont pas été suivis d'effet ou que les suites qui y ont été données sont insuffisantes.

L'argument de la garantie juridictionnelle *a posteriori* est sans doute juridiquement recevable mais stratégiquement fort compliqué. En admettant que l'argument des finalités de la loi prime sur celui du degré d'atteinte aux libertés - pour le dire autrement, que la compétence du juge judiciaire soit écartée -, le caractère seulement facultatif de l'avis de la CNCTR est difficilement acceptable. Au-delà de la logique et la cohérence du droit, il jette sur la loi le voile de la suspicion forte et légitime : c'est au Premier ministre

qu'appartient le mot le plus important. En vertu de l'article L. 821-1 du CSI, la mise en oeuvre des techniques de recueil de renseignement est soumise à autorisation préalable du Premier ministre, délivrée après avis de l'AAI. L'avis défavorable doit être motivé mais n'entraîne aucune conséquence sur la délivrance de l'autorisation. En contrepartie, la Commission peut adresser des recommandations et saisir le Conseil d'Etat.

Par ailleurs, la loi prévoit que le Premier ministre peut même passer outre la demande d'avis de la Commission « en cas d'urgence absolue » (art. L. 821-5) - à ne pas confondre avec « l'urgence opérationnelle » de l'article L. 821-6. Placée sous le contrôle du Conseil d'Etat, l'urgence absolue, dont la CNCTR est malgré tout « informée sans délai », est réservée aux finalités relatives « à la prévention d'atteintes particulièrement graves à l'ordre public » et ne peut concerner le recueil des données en temps réel sur les réseaux des opérateurs de télécommunications et les controversés algorithmes. Conditions qui ont permis au Conseil constitutionnel de ne pas censurer cette procédure d'urgence, comme le lui demandaient les députés requérants. Applicable en cas de « menace imminente » ou de « risque très élevé de ne pouvoir effectuer l'opération ultérieurement », la procédure d'urgence opérationnelle était encore plus dérogatoire que celle de l'urgence absolue, l'autorisation du Premier ministre n'étant même pas exigée. Curieusement, ce n'est pas à la demande des députés mais du Président de la République que le Conseil constitutionnel a examiné cette procédure et qu'il l'a, fort logiquement, censurée. Dépourvue de toute garantie de procédure, elle revenait, dans les faits, à donner un pouvoir excessif aux services de renseignement, notamment pour la pose des *IMSI-catchers*, portant ainsi « une atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances » (consid. 29).

B. Le choix américain d'une juridiction spéciale

Ce choix est bien antérieur à l'adoption du *Freedom Act*, qui a tenté de rendre la procédure juridictionnelle plus transparente. Le fait que, dans l'absolu, nous soyons favorable à l'intervention du juge judiciaire en amont de toute procédure de surveillance (et même si certains députés, face à une telle position, ont répondu « on n'a pas le temps ! » : réponse de J.-Y. Le Drian à C. Goasguen, Ass. nat., séance du 13 avr. 2015) n'importe pas ici. Conformément à notre regret, formulé au début de cette étude, sur l'absence du cantonnement de la loi à la lutte contre le terrorisme, nous pensons que la création d'un juge spécifique - qui existe en réalité déjà - est nécessaire à la prévention d'événements tout aussi spécifiques, dans un monde devenu différent. Ce qui ne signifie évidemment pas une nouvelle conception des libertés qui serait restrictive, mais une façon déterminée de lutter contre le terrorisme sous toutes ses formes, en assortissant ladite lutte de garanties de protection des libertés renforcées. Et de toutes les garanties, la protection judiciaire est, à nos yeux, la plus forte. Les limites entre la prévention et la répression sont si floues en ce domaine que la distinction entre police administrative et judiciaire nous paraît artificielle. Les actes de terrorisme sont des infractions autonomes punies de peines aggravées (C. pén., art. 421-1), qui obéissent à un régime procédural particulier (centralisation des poursuites, de l'instruction, jugement par une juridiction composée de magistrats spécialisés). La spécificité de ce domaine, l'exigence du niveau de spécialisation des acteurs ont été affinées à chaque étape du mouvement législatif de prévention et répression du terrorisme, de 1986 à 2012 : les services de renseignement et de police se sont spécialisés, de même que le parquet (création de la section antiterroriste du parquet de Paris disposant d'une compétence nationale). Le renseignement n'échappe pas à la règle de la spécialisation des acteurs, bien au contraire : l'analyse des techniques de renseignement fait ressortir leur aspect hautement sophistiqué, et il est fort inquiétant que la loi du 24 juillet n'exige le critère de la compétence technique que pour un seul membre de l'AAI censée être la gardienne des libertés. Si les finalités de la loi n'avaient pas été aussi

larges et imprécises mais plutôt resserrées sur celle de la lutte contre le terrorisme, la cohérence aurait permis l'exigence d'une autorisation délivrée, non par une commission, mais par un juge spécialiste des questions relatives au renseignement et à la lutte contre le terrorisme. L'argument de la réactivité (« on n'a pas le temps d'appeler le procureur ! ») avancé lors des débats parlementaires est faible : en quoi une AAI composée de neuf personnes dont certaines n'ont aucune expérience dans ce domaine serait-elle plus rapide et efficace qu'un juge spécialisé ? Les discussions actuelles autour de la « non-nomination » de M. Jean-Marie Delarue, président de la Commission nationale de contrôle des interceptions de sécurité, prouvent la nécessité d'élever des questions aussi fondamentales - vitales - pour notre Nation au-dessus de toute autre contingence.

Pour cette raison, la délivrance des autorisations pour la mise en oeuvre de techniques aussi sophistiquées et intrusives de surveillance devrait être du ressort non du pouvoir exécutif mais de celui d'un juge doté de cette seule compétence. Ou, *a minima*, du ressort du pouvoir exécutif mais après autorisation, et non seulement avis, dudit juge. Ce modèle proposé est bien évidemment comparable au mandat délivré par la *FISA Court* en matière de surveillance aux Etats-Unis. Mais les événements récents, que le *Freedom Act* ne parviendra pas - du moins, pas dans l'immédiat - à oublier ne donnent pas vraiment bonne réputation à ce système.

Le *Freedom Act* tente ainsi d'apporter plus de transparence à la procédure devant la *FISA Court* (v., en particulier, le titre IV de la loi, *« Foreign Intelligence Surveillance Court reforms »*). Aussi la loi crée-t-elle un nouveau panel d'experts qui pourront être auditionnés par ladite Cour, dans le domaine des droits et libertés et des nouvelles technologies de communication. Par ailleurs, les principales décisions de la Cour seront prononcées en public, alors que l'ensemble de la procédure devant elle, depuis sa création en 1978 suite à l'affaire du *Watergate* était marquée du sceau du secret. Mais si le principe d'une telle cour spéciale nous semble intéressant à observer dans l'optique d'une éventuelle comparaison, voire transposition, tel n'est pas le cas de la pratique. Il faudra sans doute du temps aux nouvelles dispositions du *Freedom Act* relatives à la *FISA Court* pour débarrasser celle-ci du lourd fardeau d'un passé opaque, la NSA ayant pratiqué des surveillances généralisées sans le mandat judiciaire en principe exigé.

La loi française va sans doute rapidement se heurter à des problèmes concrets d'application. Les opérateurs ne risquent-ils pas d'être dépassés par l'ampleur, considérable, des données collectées ? Les services de renseignement et de police, régulièrement confrontés à l'urgence, vont-ils avoir « le temps » de distinguer entre une urgence « classique » et une urgence « absolue » ? Quel sera le sort réservé par le Premier ministre aux avis de la CNCTR ? Le Conseil d'Etat ne risque-t-il pas d'être submergé par des demandes paranoïaques ? Le dernier article de la loi indique que toutes ses dispositions feront « l'objet d'une évaluation de leur application par le Parlement dans un délai maximal de cinq ans après son entrée en vigueur ». Le rôle du chercheur n'est pas d'avoir un réflexe critique systématique mais d'éclairer sur les fausses comparaisons établies et les failles que lui paraît présenter une loi. L'option de finalités extrêmement larges et imprécises, tout comme « l'évacuation » de la question des surveillances internationales et le choix de l'autorisation préalable par une AAI n'emportent pas notre conviction. Mais le rôle du citoyen est de souhaiter et d'espérer la réussite des choix de ses représentants.

Notes de bas de page

(1) Francis Delon (proposé par le vice-président du Conseil d'Etat) est nommé président de la Commission

nationale de contrôle des techniques de renseignement ; Patrick Puges est nommé membre de la Commission en qualité de personnalité qualifiée pour ses connaissances en matière de communications électroniques. Sont en outre nommés Jacqueline de Guillenchmidt (par le vice-président du Conseil d'Etat) ; Franck Terrier et Christine Penichon (conjointement par le premier président et par le procureur général de la Cour de cassation) ; Pascal Popelin et Catherine Vautrin (par l'Assemblée nationale) ; Michel Boutant et Catherine Troendle (par le Sénat).

(2) C'est l'un des arguments du mémoire en réplique des députés auteurs de la saisine du Conseil constitutionnel : « Rien ne serait pire qu'au détour d'un texte dont l'objet principal est de lutter contre la criminalité la plus odieuse et les barbares des temps modernes, s'insinuent au coeur de notre démocratie les prémices d'une gouvernance algorithmique dont tout le monde doit craindre qu'elle échappe un jour à ses concepteurs ».